Deutscher Bundestag **Drucksache 18/10759**

18. Wahlperiode 22.12.2016

Vorabfassung - wird durch die lektorierte Version ersetzt.

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/10467 –

Angeblich geplante Cyberangriffe der russischen Regierung auf die Bundestagswahl

Vorbemerkung der Fragesteller

Laut der „Frankfurter Allgemeine“ Zeitung wollen „russische Geheimdienste“ die Bundestagswahl im kommenden Jahr „durch Cyber-Angriffe beeinträchtigen“ (FAZ vom 10. November 2016). Auch Sabotage-Akte gegen kritische Infrastrukturen, darunter die Strom- und Wasserversorgung, seien möglich. Bereits in den US-amerikanischen Wahlkampf hätten sich „russische „Geheimdienste“ eingemischt. Auch der britische Geheimdienst werfe Moskau vor, mit „aller Macht und der Fülle seiner Staatsorgane in zunehmend aggressiver Weise außenpolitische Interessen durchzusetzen – unter Verwendung von Propaganda, Spionage, Cyber-Attacken und Umstürzen“. In Deutschland seien sogar „massive Angriffe“ zu erwarten, die jetzige politische Führung kenne „da nur ganz wenige Grenzen“. Drei Jahre nach der Bundestagswahl will Russland laut der „FAZ“ „eine schlagkräftige Cyber-Armee“ in die neue russische Militärstrategie eingliedern. Die Zahl der Kräfte, die in Russland für den Geheimdienst FSB als „Hacker und Spezialisten in Laboren“ an Cyber-Attacken arbeiteten, schätzt die „FAZ“ auf 10 000 Personen. Aufträge würden auch an „Hacker aus der organisierten Kriminalität“ vergeben. Belege oder Quellen für ihre Behauptungen nennt die Zeitung nicht, sondern beruft sich auf nicht näher genannte „Sicherheitskreise“.

Auf ähnliche Weise äußerten sich die Chefs zweier deutscher Geheimdienste, Dr. Hans-Georg Maaßen (Bundesamt für Verfassungsschutz) und Gerhard Schindler (Bundesnachrichtendienst), gegenüber dem „FOCUS“ in einem Interview mit dem Reporter Josef Hufelschulte (16. April 2016), das von dem Blatt mit „Nach diesem Interview werden Sie nicht ruhiger schlafen“ betitelt wird. Laut Gerhard Schindler seien „die Russen“ sehr gut darin, „psychologische Operationen“ durchzuführen. Ziele seien die Ukraine, die baltischen Staaten und „Westeuropa insgesamt“. Der Kreml nutze „jede Gelegenheit“, um Deutschland zu diskreditieren: „Desinformation, Infiltration, Einflussnahme, Propaganda und Zersetzung. Das sind Maßnahmen, die der KGB schon zu Sowjetzeiten hervorragend beherrschte“. Dies betreffe auch deutsche „Mitarbeiter der Parlamentarier oder politischer Stiftungen“, es habe diesbezüglich „eine erhebliche Reihe von Anbahnungsversuchen“ gegeben. Auch der Whistleblower

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 21. Dezember 2016 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Vorabfassung - wird durch die lektorierte Version ersetzt.

Edward Snowden arbeite für die russische Regierung, als Beleg nennt Gerhard Schindler dass es „sehr auffällig“ sei, dass Edward Snowden „ausgerechnet Unterlagen über die Zusammenarbeit der NSA mit dem BND oder dem englischen Geheimdienst GCHQ veröffentlicht hat“. Ebenfalls auffällig sei, dass es keine Veröffentlichungen zu Ländern wie China oder Russland gebe. Belege für seine Behauptungen nennt der BND-Chef nicht. Dazu befragt gibt auch die Bundesregierung zu, dass es keine belastbaren Erkenntnisse „über die genauen Motive des Handelns von Edward Snowden“ gebe (Bundestagsdrucksache 18/8631).

Bereits im Februar 2016 berichtete der Journalist Georg Mascolo über Ermittlungen des Bundesnachrichtendienstes (BND) und des Bundesamtes für Verfassungsschutz (BfV), dass die russische Regierung „gezielt Desinformationen in Deutschland streut, um die öffentliche Meinung zu beeinflussen und Deutschland so systematisch zu destabilisieren“ (tagesschau.de vom 18. Februar 2016). Wie in der „FAZ“ und im „FOCUS“ finden sich auch in der „Süddeutschen Zeitung“ keine Quellen oder Belege. Laut Georg Mascolo lasse das Kanzleramt nun aber ermitteln, „ob die russische Regierung mit geheimdienstlichen Mitteln die politische Debatte und die öffentliche Meinung in Deutschland zu beeinflussen sucht“. Beauftragt seien damit der BND und das BfV, auch das Auswärtige Amt sei „informiert und eingebunden“. Die „nun laufenden Ermittlungen“ würden von dem für die Geheimdienste zuständigen Staatssekretär im Bundeskanzleramt Klaus-Dieter Fritsche beaufsichtigt. Auf Nachfrage erklärt Klaus-Dieter Fritsche, ein gemeinsamer Bericht des BND und des BfV zu dieser Fragestellung sei in Auftrag gegeben worden, liege aber noch nicht in seiner abschließenden Form vor (Bundestagsdrucksache 18/10313). Angaben zu Ergebnissen „und etwaig daraus resultierenden Maßnahmen“ seien deshalb nicht möglich.

Vorbemerkung der Bundesregierung

1. Die Beantwortung der Fragen 6 und 12 kann aus Gründen des Staatswohls nicht in offener Form erfolgen. Die unbefugte Kenntnisnahme von Einzelheiten zu Aufklärungserkenntnissen des Bundesamtes für Verfassungsschutz könnte sich nachteilig auf die Interessen der Bundesrepublik Deutschland auswirken. Aus ihrem Bekanntwerden können Rückschlüsse auf die Arbeitsweise und Methode der Nachrichtendienste des Bundes gezogen werden, die nach der Rechtsprechung des Bundesverfassungsgerichts besonders schutzbedürftig sind (BVerfGE 124, 161 (194). Hierdurch würde die Funktionsfähigkeit der Sicherheitsbehörden beeinträchtigt, was wiederum die Sicherheit der Bundesrepublik Deutschland gefährdet.

Diese Informationen werden daher als Verschlusssache gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministerium des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem VS-Grad „Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

Die Beantwortung der Frage 13a kann zum Schutz der Betroffenen teilweise nicht in offener Form erfolgen. Auch diese Antwort wird daher als Verschlusssache gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministerium des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem VS-Grad „Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

2. Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Frage 3 in Teilen aus Gründen des Staatswohls nicht offen erfolgen kann. Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sind im Hinblick auf die künftige Erfüllung des gesetzlichen Auftrags aus § 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst

(BNDG) besonders schutzwürdig. Ebenso schutzbedürftig sind Einzelheiten zu der nachrichtendienstlichen Erkenntnislage. Eine Veröffentlichung von Einzelheiten betreffend solcher Erkenntnisse würde zu einer wesentlichen Schwächung der dem Bundesnachrichtendienst (BND) zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen. Dies würde für die Auftragserfüllung des BND erhebliche Nachteile zur Folge haben. Sie kann für die Interessen der Bundesrepublik Deutschland schädlich sein. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der VSA mit dem VS-Grad „VS – Vertraulich“ eingestuft und werden in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.

1. Welche Angriffe auf digitale Infrastrukturen der Bundesregierung hat es im Jahr 2016 gegeben, die auf eine mutmaßliche oder nachgewiesene Urheberschaft von Geheimdiensten hindeuten, und um welche Angriffe bzw. Urheber handelt es sich dabei?

Elektronische Angriffe gegen digitale Infrastrukturen der Bundesregierung detektiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) aufgrund § 5 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) und informiert bei Verdacht auf einen nachrichtendienstlichen Hintergrund das Bundesamt für Verfassungsschutz (BfV) über entsprechende Angriffe.

Laut Lagebericht des BSI 2016 (s. unter www.bsi.bund.de, Publikationen, Lageberichte) hat das BSI in der ersten Jahreshälfte allein über 400 Angriffe auf Regierungsnetze pro Tag detektiert, die mit kommerziellen Schutzprodukten nicht erkannt wurden. Hierunter fallen täglich etwa 20 hochspezialisierte Angriffe, die nur durch manuelle Analysen erkannt werden konnten. Durchschnittlich einer dieser Angriffe pro Woche hatte nach Einschätzung des BSI einen nachrichtendienstlichen Hintergrund.

2. Über welche vagen oder belastbaren Hinweise verfügt die Bundesregierung zur Meldung, dass „russische Geheimdienste“ angeblich die Bundestagswahl im kommenden Jahr „durch Cyber-Angriffe beeinträchtigen“ wollen?

Die Annahme, dass russische Geheimdienste versuchen könnten, die Bundestagswahl 2017 durch Cyber-Angriffe zu beeinflussen, gründet auf Analysen der mutmaßlich russischen Cyberangriffs-Kampagnen mit internationaler Zielauswahl. Die Bundesregierung verweist insbesondere auf den im Juni 2016 bekannt gewordenen erfolgreichen Cyberangriff mit anschließendem Datendiebstahl auf das Netzwerk des Democratic National Committee (DNC), der Zentrale der Demokratischen Partei der Vereinigten Staaten. In dessen Folge wurden über 19 000 dabei erbeutete interne E-Mails des DNC auf Wikileaks veröffentlicht, was zu erheblichen innenpolitischen Verwerfungen in den USA geführt hat; u. a. trat die Parteivorsitzende der Demokraten kurz danach zurück.

Die Analysen der drei mit der Untersuchung des Angriffs beauftragten unabhängigen IT-Sicherheitsunternehmen ergaben Hinweise auf eine Infektion durch die beiden Angriffskampagnen APT 28 und APT 29, die IT-Sicherheitsunternehmen Russland zuordnen.

Vorabfassung - wird durch die lektorierte Version ersetzt.

Dass auch der parlamentarische Bereich in Deutschland im Fokus russischen Aufklärungsinteresses steht, ist spätestens seit dem erheblichen Cyberangriff auf den Deutschen Bundestag im Frühjahr 2015 ersichtlich. Im Mai und August 2016 waren erneut der Deutsche Bundestag sowie mehrere politische Parteien Ziel weiterer Cyberattacken, die der Angriffskampagne APT 28 zugerechnet werden. Bei der Angriffskampagne APT 28 deuten eine Vielzahl von Indizien auf eine russische Urheberschaft hin.

a) Welche Art von konkreten „Angriffen“ hält die Bundesregierung dabei für möglich?

Die Bundesregierung spekuliert nicht über mögliche konkrete „Angriffe“.

b) Über welche vagen oder belastbaren Hinweise verfügt die Bundesregierung zur Meldung, „russische „Geheimdienste“ hätten sich mit „Cyber-Angriffen“ auch in den US-amerikanischen Wahlkampf oder das Brexit-Votum in Großbritannien eingemischt?

Zu angeblichen russischen Cyberangriffen zur Beeinflussung des Brexit-Votums in Großbritannien liegen der Bundesregierung keine Erkenntnisse vor. Im Übrigen wird auf die Antwort zu Frage 2 verwiesen.

3. Was ist der Bundesregierung über eine angebliche „schlagkräftige Cyber-Armee“ der russischen Regierung bekannt, die ab 2020 einsatzbereit und für den Geheimdienst FSB als „Hacker und Spezialisten in Laboren“ Aufträge übernehmen soll, und worin bestehen deren wesentlichen Unterschiede zur Bundeswehr-Einheit „Computernetzwerkoperationen“ (CNO), die nach Medienberichten ebenfalls Cyberangriffe durchführen könnte (heise.de vom 23. September 2016, „Bundeswehr operiert angeblich erstmals offensiv im Cyberspace“)?

Bereits aufgrund unterschiedlicher rechtlicher Rahmenbedingungen verbietet sich ein Vergleich der Bundeswehr-Einheit „Computernetzwerkoperationen“ (CNO) mit einer russischen Cyber-Gruppe. Die übrige Teilantwort auf Frage 3 ist als Verschlusssache gemäß der VSA mit dem VS-Grad „Vertraulich“ eingestuft; sie wird bei der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden. Zur Begründung wird auf die Vorbemerkung der Bundesregierung hingewiesen.

4. Über welche vagen oder belastbaren Erkenntnisse verfügt die Bundesregierung seit der Beantwortung der Bundestagsdrucksache 18/8631 über „psychologische Operationen“ unter Zuhilfenahme von „Desinformation, Infiltration, Einflussnahme, Propaganda und Zersetzung“ durch „die Russen“ in Deutschland?

Seit der Antwort auf Bundestagsdrucksache 18/8631 liegen der Bundesregierung keine neuen Erkenntnisse vor.

5. Inwiefern wurden seit Beantwortung der Bundestagsdrucksache 18/8631 „Mitarbeiter [deutscher] Parlamentarier oder politischer Stiftungen“ angeworben oder infiltriert, wie es die Geheimdienstchefs des BND und BfV ohne Angaben von Quellen behauptet hatten?

Seit der Antwort auf Bundestagsdrucksache 18/8631 liegen der Bundesregierung keine neuen Erkenntnisse vor.

Vorabfassung - wird durch die lektorierte Version ersetzt.

Die Spionageabwehr des BfV hat jedoch in den letzten Jahren immer wieder von Kontaktaufnahmen Angehöriger russischer Nachrichtendienste zu Mitarbeiterinnen und Mitarbeitern von Mitgliedern des Bundestages verschiedener Fraktionen erfahren.

6. Inwiefern verfügt die Bundesregierung auch weiterhin nicht über belastbare Erkenntnisse, dass der Whistleblower Edward Snowden wie von den Geheimdienstchefs des BND und BfV behauptet, für die russische Regierung arbeite (Bundestagsdrucksache 18/8631)?

Die Antwort ist als Verschlusssache gemäß der VSA mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird gesondert übersandt.*

7. Welche Bundesministerien der Bundesregierung mit welchen nachgeordneten Behörden überprüfen und/oder ermitteln derzeit, „ob die russische Regierung mit geheimdienstlichen Mitteln die politische Debatte und die öffentliche Meinung in Deutschland zu beeinflussen sucht“ oder ob die russische Regierung hierzu über Helferinnen und Helfer in Deutschland verfügt?

   a) Welche Abteilungen bzw. Arbeitsgruppen wurden hierzu bei den Behörden eingerichtet, wer nimmt daran teil, und wer beaufsichtigt diese?

   b) Wie lautet die konkrete Aufgabenbeschreibung dieser Abteilungen bzw. Arbeitsgruppen?

   c) Inwiefern sind diese Abteilungen bzw. Arbeitsgruppen temporär oder auf Dauer angelegt?

8. Welche weiteren Organisationen oder Personen sind an der Abfassung eines gemeinsamen Berichts unter anderem des BND und des BfV beteiligt, der untersuchen soll „ob die russische Regierung mit geheimdienstlichen Mitteln die politische Debatte und die öffentliche Meinung in Deutschland zu beeinflussen sucht“?

   a) Wann sollte der Bericht vorliegen, wann wurde er fertiggestellt, und wann soll die Prüfung abgeschlossen sein?

   b) Wem soll der Bericht zugänglich gemacht werden?

Die Fragen 7 und 8 werden gemeinsam beantwortet.

Die Bundesregierung hat das BfV und den BND um eine gemeinsame Prüfung gebeten, ob die russische Regierung mit geheimdienstlichen Mitteln die politische Debatte und die öffentliche Meinung in Deutschland zu beeinflussen versucht. Hinweisen auf derartige Aktivitäten gehen das BfV und der BND im Rahmen ihrer jeweiligen gesetzlichen Befugnisse nach.

Innerhalb des BfV wurde dazu eine temporäre Arbeitseinheit eingerichtet. Im BND wird dieser Themenkomplex vor dem Hintergrund zahlreicher Schnittstellen inhaltlich in mehreren Arbeitsbereichen/Abteilungen bearbeitet.

Der von BfV und BND gemeinsam erstellte Bericht zu russischen Einflussaktivitäten liegt der Bundesregierung nunmehr vor. Es wurde noch nicht entschieden, welchen weiteren Stellen in und außerhalb der Bundesregierung der Bericht zugänglich gemacht werden soll. Neben dem BND und dem BfV waren keine weiteren Organisationen an der Erstellung dieses Berichtes beteiligt.

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Vorabfassung - wird durch die lektorierte Version ersetzt.

9. Sofern der Bericht bereits vorliegt und geprüft wurde, welche Ergebnisse hält die Bundesregierung für herausragend?

Die Bundesregierung wertet den Bericht derzeit aus, über Ergebnisse können daher noch keine Aussagen getroffen werden.

10. Mit welchen Maßnahmen will die Bundesregierung auf die Ergebnisse des Berichtes reagieren, etwa um zu verhindern, dass die russische Regierung „mit geheimdienstlichen Mitteln die politische Debatte und die öffentliche Meinung in Deutschland zu beeinflussen sucht“?

Da die Prüfung des Berichts noch nicht abgeschlossen ist, kann die Bundesregierung derzeit noch keine Aussage zu etwaigen Maßnahmen treffen, die sich aus den Ergebnissen des Berichts ergeben.

11. Ist der Bundesregierung die im November 2016 von der US-Denkfabrik Atlantic Council herausgegebene Studie „Die trojanischen Pferde des Kreml“ („The Kremlin’s trojan horses“) bekannt, in der ein Stefan Meister von der Deutschen Gesellschaft für Auswärtige Politik e. V. (DGAP) die „pro-russischen Schlüsselfiguren in Deutschland“ benennt?

Die Studie ist der Bundesregierung bekannt.

a) Welche eigenen Schlussfolgerungen zieht sie aus der Studie?

Direkte Schlussfolgerungen lassen sich aus Sicht der Bundesregierung aus dieser Einzelstudie nicht ableiten. Vielmehr ist die kontinuierliche Analyse unter Einbeziehung aller offenen Quellen und eine übergreifende Zusammenarbeit für den Umgang mit Bedrohungen von hoher Bedeutung. Daher wird permanent eine große Zahl von Dokumenten ausgewertet, darunter auch diese Studie.

b) Inwiefern teilt auch die Bundesregierung (unabhängig von der DGAP-Studie) die Einschätzung, dass der ehemalige Chef des Bundeskanzleramtes Ronald Pofalla, der frühere Bundeskanzler Gerhard Schröder, der Vizekanzler Sigmar Gabriel sowie die Abgeordneten der Fraktion DIE LINKE. Wolfgang Gehrcke, Andrej Hunko und Dr. Sahra Wagenknecht zu den „pro-russischen Schlüsselfiguren in Deutschland“ gehören, und inwiefern werden die genannten Personen deshalb vom BND oder dem BfV beobachtet?

Die genannten Personen werden weder vom BfV noch vom BND beobachtet.

c) Mit welchen Bundesmitteln wird die DGAP unterstützt?

Die Deutsche Gesellschaft für Auswärtige Politik (DGAP) ist institutioneller Zuwendungsempfänger des Bundes und wurde aus dem Einzelplan des Auswärtigen Amts in 2016 mit 856 000 Euro gefördert. Daneben erhielt die DGAP auch projektbezogene Förderungen.

Vorabfassung - wird durch die lektorierte Version ersetzt.

12. Über welche vagen oder belastbaren Erkenntnisse verfügt die Bundesregierung zu Urhebern eines Cyberangriffs, der über den Internetdienstleister Dyn amerikanische Internetkonzerne wie Netflix, Twitter, Paypal und Amazon für einige Stunden blockierte und für den erstmals internetfähige Haushaltsgeräte genutzt wurden (DIE WELT vom 23. Oktober 2016, „Diese Attacke war der Testlauf einer mächtigen Cyberwaffe“), und welche Bundesbehörden untersuchen den Vorfall?

Die Antwort ist als Verschlusssache gemäß der VSA mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird gesondert übersandt.*

13. Welche Bundesministerien der Bundesregierung bzw. deren nachgeordnete Behörden ermitteln derzeit wegen welchen Verstoßes (etwa wegen Spionageverdachts), inwiefern US-Geheimdienste Server der Universität Rostock oder Bundeswehr nutzte, um Cyber-Operationen oder „Spionageangriffe zu starten oder zu steuern“ (DIE WELT vom 1. November 2016, „Liefen NSA-Cyberangriffe über Bundeswehr-Computer?“)?

Am 31. Oktober bzw. 1. November 2016 wurde über die Gruppe „Shadow Brokers“ eine Liste von Servernamen inklusive IP-Adressen publiziert, welche angeblich aus einem Datendiebstahl der Hackergruppe „Equation Group“ stammen. Derzeit gibt es keine Ermittlungen von Bundesbehörden im Sinne der Fragestellung. Das Bundeskriminalamt (BKA) führt im Auftrag des Generalbundesanwalts beim Bundesgerichtshof (GBA) lediglich einen Prüfvorgang im Zusammenhang mit den Aktivitäten der „Equation Group“ in Deutschland.

a) Welche der von der Hackergruppe „The Shadow Brokers“ veröffentlichten Liste von IP-Adressen können Servern in Deutschland zugeordnet werden?

Auf der Liste sind auch drei Server der Universität der Bundeswehr München aufgeführt. Allen Servern gemeinsam war die Nutzung des Betriebssystems Sun Solaris. Die Systeme wurden regelmäßig aktualisiert, Hinweise zu Missbrauch dieser Systeme sind für den genannten Zeitraum nicht bekannt. Sollten die Meldungen zutreffen, wäre das wissenschaftliche Netz der Universität betroffen gewesen, welches keine Verbindung zum Bundeswehrnetz hatte und hat.

Die betreffenden Systeme sind – aufgrund routinemäßiger Systemaktualisierungen und damit dem Austausch gegen neue Komponenten – seit mindestens zehn Jahren nicht mehr in Betrieb.

Die weitere Teilantwort ist als Verschlusssache gemäß der VSA mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird gesondert übersandt.*

b) Welche der betroffenen deutschen Einrichtungen haben nach Kenntnis der Bundesregierung bereits Strafanzeige erstattet?

Der Bundesregierung liegen bis jetzt weder Strafanzeigen im Zusammenhang mit den Veröffentlichungen „The Shadow Brokers“ vor noch ist bekannt, dass solche gestellt wurden.

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Vorabfassung - wird durch die lektorierte Version ersetzt.

c) Inwiefern wurden die betroffenen Server von Bundesbehörden forensisch untersucht?

Die Bundeswehr hat die Berichterstattung zu einem möglichen Missbrauch von Servern der Bundeswehr Universität (UniBw) München zur Kenntnis genommen. Da die in der Berichterstattung erwähnten Systeme seit zehn Jahren nicht mehr in Betrieb sind (siehe Antworten zu den Fragen 13 und 13a) und keine Backups aus den vorherigen Betriebsperioden existieren, liegen keine forensisch prüfbaren Grundlagen zur objektiven Bewertung der Vermutungen vor.

Es gibt unter Berücksichtigung aller bekannten Fakten derzeit keinerlei Hinweise darauf, dass diese Server tatsächlich kompromittiert oder gar für weitere Angriffe missbraucht wurden.

d) Welche ersten Ergebnisse etwaiger Ermittlungen kann die Bundesregierung mitteilen?

Auf die Antwort zu Frage 13 wird verwiesen.

14. Sofern die Berichte zutreffen, dass tatsächlich deutsche Server für Cyber-Operationen oder „Spionageangriffe“ von US-Geheimdiensten genutzt wurden, inwiefern handelt es sich aus Sicht der Bundesregierung also um eine „hybride Bedrohung“, die von ihr dahingehend charakterisiert wird, dass deren Ausführende bemüht sind „die Urheberschaft gezielt zu verschleiern“ (Bundestagsdrucksachen 18/6989, 18/8631)?

„Hybride Bedrohungen“ können sich auf verschiedene Weise manifestieren: Die Verbindung staatlicher und nicht-staatlicher Akteure, militärischer und nicht-militärischer Mittel, asymmetrische Einsatzformen, Propaganda und Desinformation oder auch Cyberattacken und -sabotage und die Nutzung des Cyber-Informationsraums, um nur einige mögliche Elemente eines „hybriden Bedrohungsszenarios“ zu nennen.

Die Annahme einer Beteiligung von US-Geheimdiensten in einer möglichen Ausnutzung von deutschen Servern bewegt sich im spekulativen Bereich. Die Bundesregierung beteiligt sich nicht an Spekulationen.

Allein aus dem Umstand einer Verschleierung kann nicht automatisch eine hybride Bedrohung geschlussfolgert werden. Erst aus dem gezielten, koordinierten Einsatz einer Kombination von Faktoren wäre das Muster einer hybriden Bedrohung ableitbar.

a) In welchen weiteren außer den in Bundestagsdrucksache 18/8631 (Antwort zu Frage 8) genannten herausragenden Fällen hat die Bundesregierung eine „gezielte Verschleierung der Verantwortlichkeit“ in der jüngeren Vergangenheit beobachtet?

b) Inwiefern hat die Bundesregierung den Einsatz „hybrider Bedrohungen“ mittlerweile auch bei Mitgliedstaaten der NATO beobachtet (bitte nicht wie in Bundestagsdrucksache 18/8631 hypothetisch angeben, sondern – sofern überhaupt vorhanden – belastbare Erkenntnisse mitteilen)?

Die Fragen 14a und 14b werden zusammen beantwortet.

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

Vorabfassung - wird durch die lektorierte Version ersetzt.

15. Welche Medienprojekte „mit einem Bezug zu Russland“ wurden nach Kenntnis der Bundesregierung im Jahr 2016 mit 2,3 Mio. Euro bei der Umsetzung des EU-Aktionsplans über „strategische Kommunikation“ gefördert (Bundestagsdrucksache 18/8631)?

Die Umsetzung des EU-Aktionsplans über strategische Kommunikation erfolgt zum einen durch den Europäischen Auswärtigen Dienst und die Europäische Kommission. Zusätzlich gibt es unterstützende Maßnahmen der Bundesregierung und anderer EU-Mitgliedstaaten.

16. Was ist der Bundesregierung über Pläne bekannt, die „Task Force für strategische Kommunikation“ (EU EAST STRATCOM) der Europäischen Union personell aufzustocken und ihr Aufgaben- bzw. Tätigkeitsspektrum zu erweitern (Bundestagsdrucksache 18/9388)?

Im aktuellen Haushaltsverfahren der EU gab es Bemühungen des Europäischen Parlaments, u. a. die Task Force STRATCOM EAST des Europäischen Auswärtigen Dienstes deutlich personell aufzustocken und mit einem eigenen Budget auszustatten. Diese haben sich jedoch nicht durchgesetzt.

Darüber hinaus sind der Bundesregierung keine konkreten Pläne für eine Aufstockung bzw. Aufgabenausweitung der Task Force STRATCOM EAST bekannt.

17. Auf welche Weise wird die Bundesregierung die „Schlussfolgerungen des Rates zur Bewältigung hybrider Bedrohungen“ vom 19. April 2016 (Ratsdokument 7928/16) berücksichtigen und/oder umsetzen, der ein „rasches und angemessenes Handeln zur Prävention und Bewältigung von hybriden Bedrohungen für die Union und ihre Mitgliedstaaten sowie für ihre Partner“ anmahnt?

Die Bundesregierung begrüßt die Schlussfolgerungen des Rates zur Bewältigung hybrider Bedrohungen ausdrücklich und betrachtet diese auch als Bekräftigung zur Umsetzung der Maßnahmen des Gemeinsamen Rahmens für die Abwehr hybrider Bedrohungen vom 6. April 2016 ohne sich dabei jede Einzelmaßnahmen zu eigen zu machen.

Die Bundesregierung verfolgt in der Abwehr/Bewältigung hybrider Bedrohungen einen ressortgemeinsamen Ansatz.

18. Sofern sich die ressortübergreifende Ableitung der Bundesregierung zu den in den Schlussfolgerungen angeregten Maßnahmen weiterhin erst im Anfangsstadium befindet, wann sollen Details zur Umsetzung vorliegen?

Kommission und Hohe Vertreterin zählen in der Gemeinsamen Mitteilung vom 6. April 2016 insgesamt 22 Maßnahmen auf, die sie als ganzheitlichen Ansatz vorschlagen, der es der EU ermöglichen soll, in Abstimmung mit den Mitgliedstaaten Bedrohungen hybrider Natur abzuwehren. Die Bundesregierung hat mit einer Bestandsaufnahme der bereits existierenden Vorkehrungen begonnen.

Die Bundesregierung geht davon aus, dass die Hohe Vertreterin bis Juli 2017 der Bitte des Rates entsprechen wird, einen Bericht zur Bewertung der Fortschritte vorzulegen.

Im Übrigen wird auf die Antwort zu Frage 17 wird verwiesen.

Vorabfassung - wird durch die lektorierte Version ersetzt.

19. Welche weiteren Details zur „EU Hybrid Fusion Cell“, die derzeit vom Europäischen Auswärtigen Dienst eingerichtet wird, sind der Bundesregierung mittlerweile bekannt (Bundestagsdrucksache 18/8631)?

Die Notwendigkeit einer solchen Zelle wurde als ein Mittel in den Schlussfolgerungen des Rates der Europäischen Union zur Bewältigung hybrider Bedrohungen vom 19. April 2016 beschrieben. Die konkrete Einrichtung dieser Hybrid Fusion Cell soll im EU Intelligence Analysis Centre im Europäischen Auswärtigen Dienst erfolgen. Sie ist derzeit noch in der personellen Aufstellung.

a) Inwiefern wird auch die Bundesregierung eine nationale Kontaktstelle für die „Hybrid Fusion Cell“ einrichten, und welche Aufgaben werden dort von welchen Behörden übernommen?

Die Bundesregierung wird eine nationale Kontaktstelle für die „Hybrid Fusion Cell“ einrichten. Der nationalen Kontaktstelle wird die Verteilung von Nachrichten der „Hybrid Fusion Cell“ innerhalb der Bundesregierung zugewiesen. Im Übrigen wird auf die Antworten zu den Fragen 18 und 19 verwiesen.

b) Was ist der Bundesregierung mittlerweile darüber bekannt, inwiefern die „Hybrid Fusion Cell“ mit einer NATO-Abteilung gegen „hybride Bedrohungen“ gemeinsame Übungen „auf politischer und technischer Ebene“ durchführen will, und welche parallelen oder gemeinsamen Übungen sind bereits ausformuliert?

Die Außenminister der NATO und der Rat der EU haben am 6. Dezember 2016 ein „Gemeinsames Vorschlagspaket“ (Common Set of Proposals) indossiert, um die „Gemeinsame Erklärung“ des Präsidenten des Europäischen Rates, des Kommissionspräsidenten und des NATO-Generalsekretärs vom 8. Juli 2016 umzusetzen. Für die Zusammenarbeit zwischen der „EU Hybrid Fusion Cell“ und den entsprechenden NATO-Ansprechpartnern sieht das Vorschlagspaket einen verbesserten Informationsaustausch auf Arbeitsebene u. a. zu potentiellen hybriden Bedrohungen vor.

Die Umsetzung der Joint Declaration von Warschau, u. a. im Hinblick auf Übungen, befindet sich derzeit in der Abstimmung zwischen den beiden Organisationen.

20. Wie viele Personen sind mit welcher Aufgabenbeschreibung bei der NATO in der neuen „Abteilung für Nachrichtenwesen und Sicherheit“ tätig (Schriftliche Frage 22 der Abgeordneten Inge Höger auf Bundestagsdrucksache 18/10358)?

a) Inwiefern ist mittlerweile geklärt, „ob und wie die neue Abteilung für Nachrichtenwesen und Sicherheit“ mit anderen Geheimdiensten oder geheimdienstlichen Lagezentren, darunter dem „Zentrum für Informationsgewinnung und Analyse der Europäischen Union“ (INTCEN) oder dem EU Military Staff (EUMS) zusammenarbeiten wird?

Vorabfassung - wird durch die lektorierte Version ersetzt.

b) Auf welche Weise grenzt sich die Arbeit der neuen „Abteilung für Nachrichtenwesen und Sicherheit“ von dem am 1. September 2015 eingerichteten EU-Team für „Strategische Kommunikation“ ab (Antwort von Vizepräsidentin Mogherini im Namen der Kommission auf die Anfrage der EU-Abgeordneten Sabine Lösing, Kommissionsdokument E-002156/2016)?

Die Fragen 20, 20a und 20b werden gemeinsam beantwortet.

Die Abteilung für Nachrichtenwesen und Sicherheit im Internationalen Stab der NATO befindet sich im Aufbau. Im Übrigen wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 22 der Abgeordneten Inge Höger vom 8. November 2016 verwiesen (Bundestagsdrucksache 18/10358). Die Bundesregierung äußert sich nicht zu Detailfragen hinsichtlich der Personalstärke und Aufgabenbeschreibung der Verwaltungsapparate Dritter.

21. Welche neueren Erkenntnisse hat die Bundesregierung darüber, ob bzw. wo es bis heute einen versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlag“ gegeben hat, bzw. liegen ihr hierzu nach wie vor keine Informationen darüber vor, dass es eine derartige, nicht von Staaten ausgeübte versuchte oder erfolgreich ausgeführte Attacke jemals gegeben hat (Bundestagsdrucksachen 17/7578, 18/164)?

Aus dem Phänomenbereich der politisch motivierten Kriminalität liegen der Bundesregierung derzeit keine Erkenntnisse über einen versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlag“ gegen die Bundesrepublik Deutschland vor.

Insbesondere sind aus dem Phänomenbereich „Islamismus und islamistischer Terrorismus“ derzeit keine Vorfälle bekannt, die unter den Begriff „cyberterroristischer Anschlag“ fallen. Gleichwohl gab es und gibt es auch gegenwärtig weltweit eine Vielzahl an elektronischen Operationen, die Islamisten zuzurechnen sind, z. B. die Veränderung bestehender Internetauftritte zu Propagandazwecken (sog. Defacements).

Vorabfassung - wird durch die lektorierte Version ersetzt.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333